Del 11 al 20 de julio

AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN, JASANGARRITASUN ETA INGURUMEN SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIDAD Y MEDIO AMBIENTE

GRUPO spri TALDEA

Basque CyberSecurity Centre

Vulnerabilidad zero-day en Apple

Apple ha publicado diversos avisos de seguridad, en los que se aborda una vulnerabilidad, cuyo identificador es CVE-2023-37450, que afecta a las últimas versiones de los sistemas operativos iOS, iPadOS, macOS Ventura y el navegador Safari para macOS Big Sur y Monterey. El fallo se debe a errores existentes en el componente WebKit y de momento no tiene asignada una puntuación de acuerdo con la escala CVSSv3, pero ha sido calificada por el fabricante como de tipo zero-day, por lo tanto, se les asigna una severidad crítica.

Avisos técnicos - Del 11 al 20 de julio

Actualización de seguridad de Microsoft-Julio 2023

Microsoft ha publicado las actualizaciones de seguridad del mes de julio de 2023 en las que se corrigen 131 vulnerabilidades, siendo 9 de ellas calificadas como críticas y 122 como importantes. Dentro de ellas existen 5 zero-day, CVE-2023-32049, CVE-2023-35311, CVE-2023-32046, CVE-2023-36874, que están siendo explotadas y la CVE-2023-36884 que ha sido divulgada y explotada.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidad crítica en FortiOS y FortiProxy

Fortinet ha publicado un aviso de seguridad donde se corrige una vulnerabilidad crítica que afecta a los productos FortiOS y FortiProxy cuyo identificador es CVE-2023-33308. El error puede permitir que un atacante remoto pueda ejecutar código o comandos arbitrarios a través de paquetes manipulados y, de ser explotado, representa una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidad RCE en Citrix Secure Access

Rilke Petrosky, investigador de F2TC Cyber Security, ha reportado una vulnerabilidad crítica en Citrix Secure Access, cuya explotación podría permitir la ejecución de código remoto (RCE).

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidad de desbordamiento de pila en productos de Fortinet

Watchtowr ha reportado a Fortinet una vulnerabilidad de severidad crítica, cuya explotación podría permitir a un atacante ejecutar código o comandos no autorizados.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidades en Citrix ADC y Citrix Gateway

Citrix ha publicado dos avisos de seguridad, CTX564169 y CTX561480, donde se tratan dos vulnerabilidades, CVE-2023-24492 de severidad crítica y CVE-2023-24491 de severidad alta, que afectan a los productos Citrix ADC y Citrix Gateway. Los fallos producen condiciones de ejecución remota de código y escalada de privilegios y, de ser explotados, podrían suponer una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 11 al 20 de julio

Actualización de seguridad de SAP de julio de 2023

SAP ha publicado varias actualizaciones de seguridad en diferentes productos en su comunicado mensual.

Avisos técnicos - Del 11 al 20 de julio

Actualizaciones de seguridad de Microsoft de julio de 2023

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 11 de julio, consta de 132 vulnerabilidades (con CVE asignado), calificadas como: 5 de severidad crítica y 127 importantes. Adicionalmente, se han publicado 2 avisos de seguridad (con códigos ADV230001 y ADV230002).

Avisos técnicos - Del 11 al 20 de julio

Actualización de seguridad de SAP-Julio 2023

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de julio para una amplia gama de sus productos. En total, se han notificado 16 nuevas notas de seguridad, a las que se añaden 2 actualizaciones de notas publicadas con anterioridad. De todas ellas, 2 se clasifican como de severidad crítica, 7 alta y 9 medias, corrigiendo fallos de denegación de servicio, Cross-Site Scripting (XSS), corrupción de memoria e inyección de comandos del sistema operativo, entre otros.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidad crítica en Cisco SD-WAN vManage

Cisco ha publicado un aviso de seguridad donde se aborda una vulnerabilidad crítica, con el identificador CVE-2023-20214, que corrige un fallo en la validación de autenticación de solicitudes para la API REST del software Cisco SD-WAN vManage. La explotación exitosa de la misma supone una amenaza de alta gravedad para la confidencialidad e integridad de los sistemas afectados.

Avisos técnicos - Del 11 al 20 de julio

Acceso no autenticado a REST API en Cisco SD-WAN vManage

Se ha identificado una vulnerabilidad de severidad crítica que afecta al producto SD-WAN vManage de Cisco, cuya explotación podría permitir a un atacante, remoto y no autenticado, obtener permisos de lectura o permisos de escritura limitados en la configuración de una instancia de Cisco SD-WAN vManage afectada.

Avisos técnicos - Del 11 al 20 de julio

Múltiples vulnerabilidades en SonicWall GMS/Analytics

SonicWall, en colaboración con NCCGroup, ha publicado 15 vulnerabilidades que afectan a su producto GMS/Analytics, 4 de ellas de severidad crítica, 4 altas y 7 medias, que podrían permitir a un atacante eludir la autenticación y exponer de información sensible a un actor no autorizado.

Avisos técnicos - Del 11 al 20 de julio

Limitación incorrecta de una ruta a un directorio restringido en ConacWin de Setelsa Security

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a ConacWin, de Setelsa Security, una plataforma de control de acceso, la cual ha sido descubierta por Black_Giraffe.

Avisos técnicos - Del 11 al 20 de julio

Limitación incorrecta de una ruta a un directorio restringido en ConacWin CB de Setelsa Security

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a ConacWin CB, de Setelsa Security, una plataforma de control de acceso, la cual ha sido descubierta por Agustín Picazo (Black Giraffe).

Avisos técnicos - Del 11 al 20 de julio

Autorización incorrecta en Apache Pulsar

Michael Marshall, investigador de DataStax, ha reportado una vulnerabilidad crítica que afecta a Apache Pulsar, cuya explotación podría permitir una escalada de privilegios.

Múltiples vulnerabilidades en productos de Juniper

Se han detectado han detectado 22 vulnerabilidades, 3 de ellas de severidad crítica y el resto medias y altas que podrían permitir un posible escape de shell en los componentes Lint y CommonLogger de Rack o un uso de memoria después de ser liberada.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidades en productos SonicWall

SonicWall, conocida empresa estadounidense de ciberseguridad, ha lanzado un anuncio de seguridad en el que se destacan ocho vulnerabilidades, cuatro de ellas catalogadas con una severidad crítica, y otras cuatro puntuadas con una criticidad alta. Dichos fallos afectan a los productos SonicWall GMS y SonicWall Analytics.

Avisos técnicos - Del 11 al 20 de julio

Oday Cross-Site Scripting en Zimbra Collaboration Suite

La vulnerabilidad detectada podría afectar a la confidencialidad e integridad de los datos.

Avisos técnicos - Del 11 al 20 de julio

Limitación incorrecta de una ruta a un directorio restringido en Aqua eSolutions

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a Aqua Drive, la cual ha sido descubierta por Ander Martínez, de Titanium Industrial Security.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidades en firewalls y controladores WLAN de Zyxel

Zyxel ha publicado un aviso de seguridad en el que se corrigen múltiples vulnerabilidades, de severidad alta, que cuentan con los identificadores CVE-2023-28767, CVE-2023-33011, CVE-2023-33012, CVE-2023-34138, CVE-2023-34139, CVE-2023-34141. También se aborda un fallo de severidad media cuyo identificador es CVE-2023-34140.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidad de inyección SQL en Ap Page Builder de LeoTheme

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a LeoTheme Ap Page Builder, la cual ha sido descubierta por David Manuel Herrera Rodríguez, del equipo de Telefónica Tech.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidades en Citrix NetScaler ADC y NetScaler Gateway

Citrix ha publicado un aviso de seguridad donde se abordan tres vulnerabilidades, CVE-2023-3519 de severidad crítica y CVE-2023-3466, CVE-2023-3467 de severidad alta, que afectan a los productos NetScaler ADC, anteriormente Citrix ADC, y NetScaler Gateway, anteriormente Citrix Gateway. Dichos errores, de ser explotados, producen condiciones de ejecución remota de código (RCE), Cross-Site-Scripting (XSS) y escalada de privilegios.

Avisos técnicos - Del 11 al 20 de julio

Múltiples vulnerabilidades en productos Citrix

Los investigadores Wouter Rijkbost y Jorren Geurts, de Resillion, han reportado 3 vulnerabilidades en productos de Citrix, una de severidad crítica y 2 altas, cuya explotación podría permitir a un atacante realizar XSS (Cross-Site Scripting), escalada de privilegios o ejecución remota de código.

Actualizaciones críticas en Oracle (julio 2023)

Oracle ha publicado una actualización crítica con parches para corregir vulnerabilidades, que afectan a múltiples productos.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidades en Google Chrome

Google ha hecho público un aviso de seguridad, anunciando una actualización del escritorio en canal estable para Google Chrome. En dicho parche, se han resuelto un total de 20 errores, teniendo 4 vulnerabilidades una severidad calificada como alta por parte de la compañía.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidades en productos de Atlassian

Atlassian ha publicado un aviso de seguridad donde se tratan 3 vulnerabilidades de severidad alta cuyos identificadores son CVE-2023-22505, CVE-2023-22508 y CVE-2023-22506. Estos errores producen condiciones de ejecución remota de código (RCE) afectando a los productos Confluence Data Center & Server y Bamboo Data Center.

Avisos técnicos - Del 11 al 20 de julio

Vulnerabilidades críticas en Adobe ColdFusion

Adobe ha publicado un aviso de seguridad en el que se abordan 3 vulnerabilidades que afectan a Adobe ColdFusion. Entre ellas se destacan 2 vulnerabilidades que han sido calificadas con una severidad crítica por parte de la compañía, siendo una de ellas explotada de manera activa en la red.

Múltiples vulnerabilidades en HelpDezk Community

INCIBE ha coordinado la publicación de 2 vulnerabilidades en HelpDezk Community, un software para la gestión de solicitudes e incidencias, que han sido descubiertas por David Utón Amaya (m3n0sd0n4ld).

Avisos técnicos - Del 11 al 20 de julio